

AMENDED IN SENATE JANUARY 28, 2008

AMENDED IN SENATE JANUARY 17, 2008

AMENDED IN SENATE JANUARY 7, 2008

SENATE BILL

No. 364

Introduced by Senator Simitian

February 20, 2007

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 364, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require the agency, person, or business, in addition to the duties specified above, to electronically report the breach to the Office of Information Security and Privacy Protection, as specified. ~~The bill would require the office to establish a Web site where an agency, person, or business shall submit electronically to the office security breach notifications meeting specified requirements and sent to California residents; the bill would require the office to make those notifications publicly available. The bill would require the office to~~

annually report a summary of the information collected and made available via the Web site to the Legislature.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of California
7 whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person, and
9 shall submit electronically any security breach notification sent to
10 California residents pursuant to this section to the Office of
11 Information Security and Privacy Protection in accordance with
12 this section. The disclosure shall be made in the most expedient
13 time possible and without unreasonable delay, consistent with the
14 legitimate needs of law enforcement, as provided in subdivision
15 (c), or any measures necessary to determine the scope of the breach
16 and restore the reasonable integrity of the data system.

17 (b) Any agency that maintains computerized data that includes
18 personal information that the agency does not own shall notify the
19 owner or licensee of the information of any breach of the security
20 of the data immediately following discovery, if the personal
21 information was, or is reasonably believed to have been, acquired
22 by an unauthorized person.

23 (c) The notification required by this section may be delayed if
24 a law enforcement agency determines that the notification will
25 impede a criminal investigation. The notification required by this
26 section shall be made after the law enforcement agency determines
27 that it will not compromise the investigation.

28 ~~(d) The Office of Information Security and Privacy Protection~~
29 ~~shall establish a Web site where agencies subject to this section~~
30 ~~shall submit electronically security breach notifications sent to~~
31 ~~California residents, and shall make these notifications publicly~~
32 ~~available online.~~

33 (e)

1 (d) A security breach notification shall meet all of the following
2 requirements:

3 (1) The security breach notification shall be provided by one of
4 the following means:

5 (A) Written notice.

6 (B) Electronic notice, if the notice provided is consistent with
7 the provisions regarding electronic records and signatures set forth
8 in Section 7001 of Title 15 of the United States Code.

9 (C) Substitute notice, if the agency demonstrates that the cost
10 of providing notice would exceed two hundred fifty thousand
11 dollars (\$250,000), or that the affected class of subject persons to
12 be notified exceeds 500,000, or the agency does not have sufficient
13 contact information. Substitute notice shall consist of any of the
14 following:

15 (i) E-mail notice when the agency has an e-mail address for the
16 subject persons.

17 (ii) Conspicuous posting of the notice on the agency's Web site,
18 if the agency maintains one.

19 (iii) Notification to major statewide media and electronic
20 submission of a *sample* copy of the security breach notification
21 ~~form or forms~~ to the Office of Information Security and Privacy
22 ~~Protection in accordance with subdivision (d)~~.

23 (2) The security breach notification shall be written in plain
24 language.

25 (3) The security breach notification shall include, at a minimum,
26 the following information:

27 (A) The toll-free telephone numbers and addresses of the major
28 credit reporting agencies.

29 (B) The name and contact information of the reporting agency.

30 (C) A list of the types of information, such as name or social
31 security number, that were or may have been the subject of a
32 breach.

33 (D) The date of a breach, if known, and the date of discovery
34 of a breach, if known.

35 (E) The date of the notification, and whether the notification
36 was delayed pursuant to subdivision (c).

37 (F) A general description of the breach incident.

38 (G) The estimated number of persons affected by the breach.

39 (H) Whether substitute notice was used.

1 ~~(4) The Office of Information Security and Privacy Protection~~
2 ~~shall annually report a summary of the information collected and~~
3 ~~made available via the Web site to the Legislature.~~

4 ~~(f)~~

5 (e) For purposes of this section, the following terms have the
6 following meanings:

7 (1) “Breach of the security of the system” means unauthorized
8 acquisition of computerized data that compromises the security,
9 confidentiality, or integrity of personal information maintained by
10 the agency. Good faith acquisition of personal information by an
11 employee or agent of the agency for the purposes of the agency is
12 not a breach of the security of the system, provided that the
13 personal information is not used or subject to further unauthorized
14 disclosure.

15 (2) (A) “Personal information” means an individual’s first name
16 or first initial and last name in combination with any one or more
17 of the following data elements, when either the name or the data
18 elements are not encrypted:

19 (i) Social security number.

20 (ii) Driver’s license number or California Identification Card
21 number.

22 (iii) Account number, credit or debit card number, in
23 combination with any required security code, access code, or
24 password that would permit access to an individual’s financial
25 account.

26 (iv) Medical information.

27 (v) Health insurance information.

28 (B) “Personal information” does not include publicly available
29 information that is lawfully made available to the general public
30 from federal, state, or local government records.

31 (3) “Medical information” means any information regarding an
32 individual’s medical history, mental or physical condition, or
33 medical treatment or diagnosis by a health care professional.

34 (4) “Health insurance information” means an individual’s health
35 insurance policy number or subscriber identification number, any
36 unique identifier used by a health insurer to identify the individual,
37 or any information in an individual’s application and claims history,
38 including any appeals records.

39 ~~(g)~~

1 (f) Notwithstanding ~~paragraphs~~ *paragraph* (1) ~~and (4)~~ of
2 subdivision ~~(e)~~ (d), an agency that maintains its own notification
3 procedures as part of an information security policy for the
4 treatment of personal information and is otherwise consistent with
5 the timing requirements of this part and paragraphs (2) and (3) of
6 subdivision ~~(e)~~ (d) shall be deemed to be in compliance with the
7 notification requirements of this section if it notifies subject persons
8 in accordance with its policies in the event of a breach of security
9 of the system.

10 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

11 1798.82. (a) Any person or business that conducts business
12 in California, and that owns or licenses computerized data that
13 includes personal information, shall disclose any breach of the
14 security of the system following discovery or notification of the
15 breach in the security of the data to any resident of California
16 whose unencrypted personal information was, or is reasonably
17 believed to have been, acquired by an unauthorized person, and
18 shall submit electronically any security breach notification sent to
19 California residents pursuant to this section to the Office of
20 Information Security and Privacy Protection in accordance with
21 this section. The disclosure shall be made in the most expedient
22 time possible and without unreasonable delay, consistent with the
23 legitimate needs of law enforcement, as provided in subdivision
24 (c), or any measures necessary to determine the scope of the breach
25 and restore the reasonable integrity of the data system.

26 (b) Any person or business that maintains computerized data
27 that includes personal information that the person or business does
28 not own shall notify the owner or licensee of the information of
29 any breach of the security of the data immediately following
30 discovery, if the personal information was, or is reasonably
31 believed to have been, acquired by an unauthorized person.

32 (c) The notification required by this section may be delayed if
33 a law enforcement agency determines that the notification will
34 impede a criminal investigation. The notification required by this
35 section shall be made after the law enforcement agency determines
36 that it will not compromise the investigation.

37 ~~(d) The Office of Information Security and Privacy Protection~~
38 ~~shall establish a Web site where any person or business subject to~~
39 ~~this section shall submit electronically security breach notifications~~

1 ~~sent to California residents, and shall make those notifications~~
2 ~~publicly available online.~~

3 (e)

4 (d) A security breach notification shall meet all of the following
5 requirements:

6 (1) The security breach notification shall be provided by one of
7 the following means:

8 (A) Written notice.

9 (B) Electronic notice, if the notice provided is consistent with
10 the provisions regarding electronic records and signatures set forth
11 in Section 7001 of Title 15 of the United States Code.

12 (C) Substitute notice, if the person or business subject to this
13 section demonstrates that the cost of providing notice would exceed
14 two hundred fifty thousand dollars (\$250,000), or that the affected
15 class of subject persons to be notified exceeds 500,000, or that the
16 person or business subject to this section does not have sufficient
17 contact information. Substitute notice shall consist of any of the
18 following:

19 (i) E-mail notice when the person or business subject to this
20 section has an e-mail address for the subject persons.

21 (ii) Conspicuous posting of the notice on the person's or
22 business' Web site, if the person or business subject to this section
23 maintains one.

24 (iii) Notification to major statewide media and electronic
25 submission of a *sample* copy of the security breach notification to
26 the Office of Information Security and Privacy Protection ~~in~~
27 ~~accordance with subdivision (d).~~

28 (2) The security breach notification shall be written in plain
29 language.

30 (3) The security breach notification shall include, at a minimum,
31 the following information:

32 (A) The toll-free telephone numbers and addresses of the major
33 credit reporting agencies.

34 (B) The name and contact information of the reporting person
35 or business subject to this section.

36 (C) A list of the types of information, such as name or social
37 security number, that were or may have been the subject of a
38 breach.

39 (D) The date of a breach, if known, and the date of discovery
40 of a breach, if known.

1 (E) The date of the notification, and whether the notification
2 was delayed pursuant to subdivision (c).

3 (F) A general description of the breach incident.

4 (G) The estimated number of persons affected by the breach.

5 (H) Whether substitute notice was used.

6 ~~(4) The Office of Information Security and Privacy Protection~~
7 ~~shall annually report a summary of the information collected and~~
8 ~~made available via the Web site to the Legislature.~~

9 (f)

10 (e) For purposes of this section, the following terms have the
11 following meanings:

12 (1) “Breach of the security of the system” means unauthorized
13 acquisition of computerized data that compromises the security,
14 confidentiality, or integrity of personal information maintained by
15 the person or business. Good faith acquisition of personal
16 information by an employee or agent of the person or business for
17 the purposes of the person or business is not a breach of the security
18 of the system, provided that the personal information is not used
19 or subject to further unauthorized disclosure.

20 (2) (A) “Personal information” means an individual’s first name
21 or first initial and last name in combination with any one or more
22 of the following data elements, when either the name or the data
23 elements are not encrypted:

24 (i) Social security number.

25 (ii) Driver’s license number or California Identification Card
26 number.

27 (iii) Account number, credit or debit card number, in
28 combination with any required security code, access code, or
29 password that would permit access to an individual’s financial
30 account.

31 (iv) Medical information.

32 (v) Health insurance information.

33 (B) “Personal information” does not include publicly available
34 information that is lawfully made available to the general public
35 from federal, state, or local government records.

36 (3) “Medical information” means any information regarding an
37 individual’s medical history, mental or physical condition, or
38 medical treatment or diagnosis by a health care professional.

39 (4) “Health insurance information” means an individual’s health
40 insurance policy number or subscriber identification number, any

1 unique identifier used by a health insurer to identify the individual,
2 or any information in an individual’s application and claims history,
3 including any appeals records.
4 ~~(g)~~
5 ~~(f)~~ Notwithstanding ~~paragraphs~~ *paragraph* (1) ~~and (4)~~ of
6 subdivision ~~(e)~~ (d), a person or business subject to this section that
7 maintains its own notification procedures as part of an information
8 security policy for the treatment of personal information and is
9 otherwise consistent with the timing requirements of this part and
10 paragraphs (2) and (3) of subdivision ~~(e)~~ (d), shall be deemed to
11 be in compliance with the notification requirements of this section
12 if the person or business notifies subject persons in accordance
13 with its policies in the event of a breach of security of the system.

O